UNITED STATES DISTRICT COURT
DISTRICT OF SOUTH DAKOTA

JACOB KENT, individually and on behalf of all others similarly situated, Plaintiff, v. PATHWARD, N.A., IPSWITCH, INC., and PROGRESS SOFTWARE CORPORATION, Defendants.	Case No. 4:23-cv-4177 **CLASS ACTION** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Jacob Kent ("Plaintiff"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to himself, and on information and belief as to all other matters, by and through undersigned counsel, brings this Class Action Complaint against Defendants Pathward, N.A. ("Pathward"), Ipswitch, Inc. ("Ipswitch"), and Progress Software Corporation ("Progress") (together, "Defendants").

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendants for their failure to secure and safeguard his and approximately 793,626 similarly situated individuals personally identifiable information ("PII"), including but not limited to names, addresses, Social Security numbers, dates of birth, driver's license numbers, email addresses, phone numbers, and debit card information.

2. Pathward is a financial institution that, among other services, provides debit cards called the H&R Block Emerald Card. Plaintiff and Class members are customers of Pathward who have used the H&R Block Emerald Card and whose PII was disclosed to unauthorized third parties during a massive data breach compromising Defendants Ipswitch and Progress's MOVEit Transfer

and MOVEit Cloud ("MOVEit") software that occurred between approximately May 27, 2023 and May 31, 2023 (the "Data Breach").

3. During the Data Breach, and due to Defendants' data security and privacy shortcomings, unauthorized persons were able to gain access to files containing the PII of Pathward's customers by exploiting a vulnerability in the MOVEit platform.

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect their PII from unauthorized access and disclosure.

5. As a result of Defendants' inadequate security measures and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all of Pathward's customers whose PII was exposed as a result of the Data Breach.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, and unjust enrichment, and seek declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Jacob Kent

7. Plaintiff Jacob Kent is a citizen of the State of Illinois.

8. Plaintiff was required to provide his PII to Pathward in connection with obtaining and using the H&R Block Emerald Card.

9. Based on representations made by Pathward relied upon by Plaintiff, Plaintiff believed that Pathward had implemented and maintained reasonable security and practices to protect his PII, including ensuring third parties it contracts with and shares PII with maintain adequate data security and practices.

10. In connection with providing banking or other financial services to Plaintiff, Pathward collected, maintained, and shared Plaintiff's PII on its systems, including the MOVEit file-transfer software.

11. Had Plaintiff known that Defendants do not adequately protect the PII in their possession, including Pathward by not ensuring that the third parties it contracts with in relation to providing banking or financial services to customers maintain adequate data security systems and practices, he would not have agreed to provide his PII to Pathward.

12. Plaintiff received a letter from Pathward notifying him that his PII was exposed in the Data Breach.

13. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, inter alia: a substantial and imminent risk of identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII; deprivation of the value of his PII; and overpayment for services that did not include adequate data security.

Defendant Pathward N.A.

14. Defendant Pathward, N.A. is a national bank that has its principal place of business in South Dakota. Pathward is headquartered at 5501 S. Broadband Lane, Sioux Falls, SD 57108.

Defendant Ipswitch, Inc.

15. Defendant Ipswitch, Inc. is a Massachusetts for profit corporation with its principal place of business located at 15 Wayside Road, 4th Floor, Burlington, MA 01803.

Defendant Progress Software Corporation

16. Defendant Progress Software Corporation is a Delaware corporation with its principal place of business located at 15 Wayside Road, Suite 4, Burlington, MA 01803.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2), because (a) there are 100 or more Class members, (b) at least one Class member is a citizen of a state that is diverse from Defendants' citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs. Further, greater than two-thirds of the Class Members reside in states other than the states in which Defendants are citizens.

18. The Court has personal jurisdiction over Pathward because it has its principal place of business in South Dakota and transacts significant business in South Dakota.

19. The Court has personal jurisdiction over Defendants Ipswitch, Inc. and Progress Software Corporation because Defendants transact significant business in South Dakota, and otherwise have sufficient minimum contacts with and intentionally avail themselves of the markets in South Dakota through their promotion, marketing, and sale of MOVEit software and other software, products, and related services.

20. Venue properly lies in this judicial district because, *inter alia,* Pathward's principal place of business is located in this District, Defendants transact substantial business in this District, and a substantial part of the conduct giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Ipswitch, Inc., Progress Software, and the Unsecure MOVEit Software

21. Ipswitch is an IT software development company founded in 1991 in Burlington, Massachusetts. Ipswitch sells its software and related products and services, including MOVEit solutions, directly and through resellers and distributors in the United States.

22. Progress, a public domestic software company based in Massachusetts, acquired Ipswitch in May 2019 for approximately $225 million.

23. Ipswitch developed and through Progress sells the MOVEit software, which they claim is "the leading secure Managed File Transfer (MFT) software used by thousands of organizations around the world to provide complete visibility and control over file transfer activities."[1]

24. On their websites, Defendants Ipswitch and Progress make a host of claims about data security and their MOVEit product. Ipswitch claims, generally, that its "Enterprise File Transfer Solutions – Mak[e] the networked world a safer place."[2] Its website states: "Our efficient, easy-to-use products empower customers to respond faster to business demands through accelerated implementation and improved productivity and security."[3]

25. Specific to MOVEit, Ipswitch claims that "MOVEit enables your organization to meet compliance standards, easily ensure the reliability of core business processes, and secure the transfer of sensitive data between partners, customers, users and systems."[4] Ipswitch claims its MOVEit Transfer and MOVEit Cloud products give customers "control" over their businesses;

---

[1] *MOVEit*, IPSWITCH, https://www.ipswitch.com/moveit (last accessed Oct. 20, 2023).

[2] *Ipswitch.com*, IPSWITCH, https://www.ipswitch.com (last accessed Oct. 20, 2023).

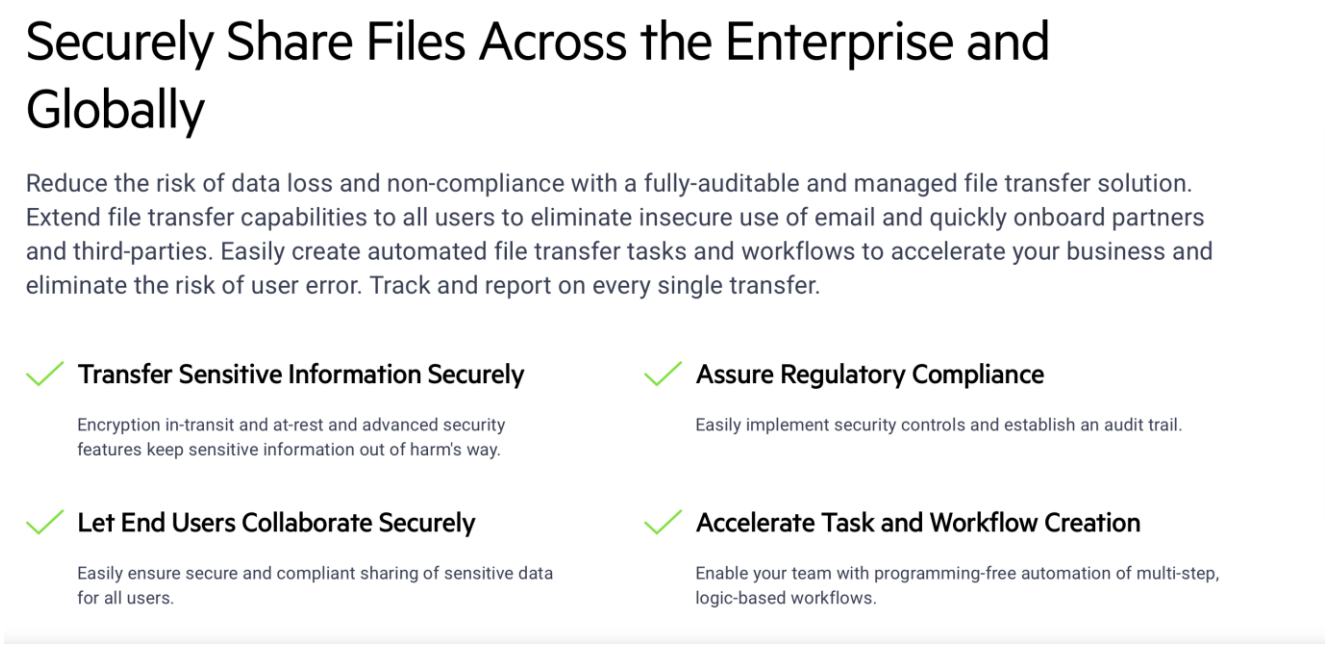
[3] *Id*.

[4] *See MOVEit*, *supra* note 1.

"provides full security, reliability and compliance"; provide "encryption, security, activity tracking tamper-evident logging, and centralized access controls to meet your operational requirements"; "[r]eliably and easily comply with SLAs, internal governance requirements and regulations like PCI, HIPAA, CCPA/CPRA and GDPR"; and provide "secure and managed file transfer."[5]

26. Progress makes similar statements about data security. Its website claims "MOVEit provides secure collaboration and automated file transfers of sensitive data" and that it provides "[e]ncryption and activity tracking enable compliance with regulations such as PCI, HIPAA and GDPR."[6]

27. Progress also touts all of the following on its website regarding MOVEit:[7]



28. As demonstrated above, Defendants Ipswitch and Progress heavily tout and promote the MOVEit products and services as capable of safely transferring sensitive information.

---

[5] *Id.*

[6] *MOVEit*, PROGRESS, https://www.progress.com/moveit (last accessed Oct. 20, 2023).

[7] *Id.*

Despite these assurances and claims, Defendants Ipswitch and Progress failed to offer safe and secure file transfer products and failed to adequately protect Plaintiff's and Class members' PII.

29. This is because the products that Defendants Ipswitch and Progress offered, and which Pathward used, were not secure. When the Data Breach occurred, there was a critical vulnerability in the MOVEit software referred to as CVE-2023-34362. Specifically, Defendants Ipswitch and Progress identified that MOVEit's web-based front end is affected by a critical structured query language (SQL) injection vulnerability/attack vector that can be exploited by an unauthenticated attacker to access databases associated with the product.

30. All of the Defendants knew or should have known that MOVEit leaves the PII of Pathward's customers, including Plaintiff and Class member, exposed to security threats. Despite this, Ipswitch and Progress continued to offer MOVEit file transfer products without adequately testing and identifying the vulnerabilities in the products, and patching or otherwise eliminating those threats.

31. Similarly, Pathward continued to use the MOVEit software without adequately ensuring it was secure and that Ipswitch and Progress had adequate data security systems and practices in place to protect Plaintiff's and Class members' PII. As one cybersecurity company noted, "Just because a piece of software claims to be 'secure' doesn't mean that it is. Customers must always validate that the software they use is secure, and is configured in a way that can protect against cyberattacks."[8]

[8] Avishai Avivi, *MOVEIt Vulnerability: A Painful Reminder That Threat Actors Aren't the Only Ones Responsible for a Data Breach*, SAFEBREACH (June 21, 2023), https://www.safebreach.com/moveit-vulnerability-a-painful-reminder-that-threat-actors-arent-the-only-ones-responsible-for-a-data-breach/.

Pathward

32. Pathward is a banking company that claims to use its "national bank charter to empower partners, and our financial expertise to deliver solutions across two business lines: Banking as a Service (BaaS), and Commercial Finance."[9]

33. Pathward provides banking services to H&R Block customers through the Spruce app and by providing the H&R Block Emerald Card.[10]

34. Pathward's website contains a privacy policy which states: "Pathward recognizes and respects the privacy of our customers who receive Services and Site visitors."[11] It goes on to state, "We take the privacy of your Personal Information seriously. We use commercially reasonable technical, administrative and physical security measures to protect your Personal Information, including generally accepted industry standards to protect the Personal Information submitted to us during transmission and once we receive it."[12]

35. The website also contains a privacy notice to United States consumers, which states, "To protect your personal information from unauthorized access and use, we use security measures that comply with federal law."[13]

---

[9] *About Us*, PATHWARD, https://www.pathward.com/about-us/ (last accessed Oct. 20, 2023).

[10] *H&R Block Financial Services*, H&R BLOCK, https://www.hrblock.com/financial-services/ (last accessed Oct. 20, 2023).

[11] *Privacy Policy*, PATHWARD, https://www.pathward.com/privacy-policy/ (last accessed Oct. 20, 2023).

[12] *Id*.

[13] *U.S. Consumer Privacy Notice*, PATHWARD, https://www.pathward.com/content/dam/pathward/us/en/documents/pdfs/GLBA-Policy-Notice.pdf (last accessed Oct. 20, 2023).

36. Some of Pathward's customers' PII was exposed in a third-party data breach less than a year prior to the Data Breach.[14] Blackhawk Engagement Solutions, which Pathward used to manage certain prepaid incentive cards, experienced a data breach on the website where it collected Pathward's customers' PII.[15] Pathward reported to the Maine Attorney General that the 2022 breach affected 165,727 persons.[16]

37. Pathward shared Plaintiff's and Class members' PII with Ipswitch and Progress via the MOVEit software in connection with providing banking or other financial services to Plaintiff and Class Members.[17] In doing so, it failed to ensure that Ipswitch and Progress implemented and maintained adequate data security practices to protect Plaintiff's and Class member's PII from unauthorized access, disclosure, and theft.

The Data Breach

38. Between approximately May 27 and May 31, 2023, unauthorized persons exploited a vulnerability in the MOVEit software to access and download files containing the sensitive PII of Plaintiff and Class Members.[18]

---

[14] *See Notice of Data Breach*, MASS.GOV, https://www.mass.gov/doc/assigned-data-breach-number-28504-pathward-na/download (last accessed Oct. 20, 2023).

[15] *See id*.

[16] *Data Breach Notifications*, OFF. OF THE ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/52a7dc3e-1734-4ea7-b1a8-6e8d49176588.shtml (last accessed Oct. 20, 2023).

[17] *See Notice of Data Security Incident*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://apps.web.maine.gov/online/aeviewer/ME/40/21df7004-999d-4dfd-bbdd-e9ea4431c2e8/3fd41d11-9893-4e69-8fc7-d1ead1757759/document.html (last accessed Oct. 20, 2023).

[18] *Id.*

39. According to reports, the Clop (also known as CLOP or Cl0p) ransomware gang is responsible for the attack on the MOVEit platform.[19]

40. On or about May 31, 2023, Progress and Ipswitch alerted their customers, including Pathward, about a critical vulnerability in the MOVEit software and the Data Breach. Despite this, Pathward waited until approximately September 27, 2023, almost four months later, to begin notifying its customers of the Data Breach.[20]

41. The Cybersecurity and Infrastructure Security Agency (CISA) and the FBI first warned on June 7, 2023, that the Clop ransomware gang was exploiting a vulnerability in MOVEit Transfer. "Internet-facing MOVEit Transfer web applications were infected with a specific malware used by CL0P, which was then used to steal data from underlying MOVEit Transfer databases," the advisory said, as it explained how threat actors carried out the attack.[21]

42. A senior CISA officer informed reporters that "several hundred" businesses and organizations in the United States may be impacted by the hacking campaign in addition to government entities.[22]

43. Plaintiff and Class members' sensitive PII was compromised in the Data Breach as a result of Ipswitch and Progress's unsecure MOVEit file transfer product being exploited by cyber

---

[19] *See Clop Gang to Earn Over $75 Million from MOVEit Extortion Attacks*, Bleeping Computer (July 21, 2023, 12:34 PM), https://www.bleepingcomputer.com/news/security/clop-gang-to-earn-over-75-million-from-moveit-extortion-attacks/.

[20] *See Notice of Data Security Incident*, *supra* note 17.

[21] Bruce Sussman, *Clop Ransomware and the MOVEit Cyberattack: What to Know*, BLACKBERRY BLOG (June 19, 2023), https://blogs.blackberry.com/en/2023/06/clop-ransomware-and-moveit-cyberattack.

[22] Onur Demirkol, *US Government Under Siege: MOVEit Breach Exposes Critical Data to Ruthless Clop Ransomware Attack*, DATA CONOMY (June 19, 2023), https://dataconomy.com/2023/06/19/moveit-breach-data-clop-ransomware/.

criminals, and because Pathward failed to ensure the third parties it contracts with to provide services to Plaintiff and Class members maintained adequate data security systems and practices.

Defendants Knew that Criminals Target PII

44. At all relevant times, Defendants knew, or should have known, that the PII that they collected was a target for malicious actors. Despite such knowledge, Defendants failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII from cyber-attacks that Defendants should have anticipated and guarded against. Pathward should have been particularly aware of the risk of providing PII to third-party vendors due to the data breach that one of its third-party vendors experienced in 2022.[23]

45. It is well known among companies that store sensitive personally identifying information that such information—such as the Social Security numbers ("SSNs") and financial information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers …. Many of them were caused by flaws in … systems either online or in stores."[24]

46. PII is a valuable property right.[25] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within

---

[23] *See Notice of Data Breach*, *supra*, n.14.

[24] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[25] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

the existing legal and regulatory frameworks."[26] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[27] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

47. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

48. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[28]

---

[26] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[27] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[28] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

49. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII Has Grave and Lasting Consequences for Victims

50. Theft of PII can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[29] [30]

51. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[31]

[29] *See* Federal Trade Commission, *What to Know About Identity Theft*, FED. TRADE COMM'N CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed Oct. 20, 2023).

[30] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 12 C.F.R. § 1022.3(g).

[31] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN (May 21, 2023), https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

52. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[32]

53. Theft of SSNs also creates a particularly alarming situation for victims because SSNs cannot easily be replaced. In order to obtain a new SSN, a breach victim has to demonstrate ongoing harm from misuse of her SSN. Thus, a new SSN will not be provided until after the harm has already been suffered by the victim.

54. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[33]

55. There may also be time lags between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.[34]

---

[32] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed Oct. 20, 2023).

[33] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

[34] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

56. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII is forever in cyberspace, having been stolen by criminals willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Damages Sustained by Plaintiff and Class Members

57. Plaintiff and Class members have suffered injury and damages, including, but not limited to: (i) a substantially increased risk of identity theft—risk which justifies or necessitates expenditures for protective and remedial services, for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face; and (vi) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

58. This action is brought and may be properly maintained as a class action pursuant to Federal Rule of Civil Procedure 23.

59. Plaintiff brings this action on his own behalf, and on behalf of the following Class of similarly situated persons:

> All persons who have an H&R Block Emerald Card through Pathward, N.A., whose personally identifiable information was accessed in the Data Breach by unauthorized persons, including all persons who have an H&R Block Emerald Card through Pathward, N.A., who were sent a notice of the Data Breach.

60. Excluded from the Class are: (i) Defendant Ipswitch, Inc. and its affiliates, parents, subsidiaries, officers, agents, directors, legal representatives, successors, subsidiaries, and assigns; (ii) Defendant Progress Software Corporation and its affiliates, parents, subsidiaries, officers,

agents, directors, legal representatives, successors, subsidiaries, and assigns; (iii) Defendant Pathward, N.A. and its affiliates, parents, subsidiaries, officers, agents, directors, legal representatives, successors, subsidiaries, and assigns; and (iv) the judge(s) presiding over this matter and the clerks of said judge(s).

61. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

62. The members of the Class are so numerous that joinder of all Class members in a single proceeding would be impracticable. Pathward reported to the Maine Attorney General that the Data Breach affected 793,626 of its customers.[35]

63. Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. Such common questions of law or fact include, inter alia:

a. whether Defendants had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII from unauthorized access and disclosure, including ensuring that the third parties it contracts with to provide services had adequate data security measures in place;

b. whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII';

c. whether an implied contract existed between Class members and Defendants, providing that Defendants would implement and maintain reasonable security measures to protect and secure Class members' PII from unauthorized access and disclosure;

[35] *Data Breach Notifications*, OFF. OF THE ME. ATT'Y GEN., https://apps.web.maine.gov/online/aeviewer/ME/40/21df7004-999d-4dfd-bbdd-e9ea4431c2e8.shtml (last accessed Oct. 20, 2023).

d. whether Defendants breached their duties to protect Plaintiff's and Class members' PII; and

e. whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

64. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of himself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

65. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

66. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

67. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for Class members to individually seek redress from Defendants' wrongful conduct. Even if Class members

could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

68. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

69. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII in their possession, custody, or control.

70. Defendants knew or should have known the risks of collecting and storing Plaintiff's and Class members' PII and the importance of maintaining secure systems, including ensuring third party vendors employed adequate data security practices. Defendants knew or should have known that they faced an increased threat of customer data theft, as judged by the many data breaches that have targeted companies that stored PII in recent years.

71. Given the nature of Defendants' businesses, the sensitivity and value of the PII they collect, store, and maintain, and the resources at their disposal, Defendants should have taken care to identify the vulnerabilities to their systems or to their third-party vendors' systems and prevented the Data Breach from occurring.

72. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage,

monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them—including Plaintiff's and Class members' PII.

73. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

74. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

75. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; (vii) loss of value of the PII that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

76. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

77. Defendants' duties arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair … practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

78. Plaintiff and Class members are the persons that the Section 5 of the FTCA was intended to protect, and the harm that Plaintiff and Class members suffered is the type of harm Section 5 of the FTCA is intended to guard against.

79. Defendants knew the risks of collecting and storing Plaintiff's and Class members' PII and the importance of maintaining secure systems, or of ensuring that third parties it contracts with and shares PII with maintain secure systems. Defendants knew of the many data breaches that targeted companies that collect, store, and share PII in recent years.

80. Given the nature of Defendants' businesses, the sensitivity and value of the PII they collect, share, and maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems, or the systems of third parties the contract with and share PII with, and prevented the Data Breach from occurring.

81. Defendants breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to, or failing to ensure the third parties they contract with and share PII with, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies,

procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them—including Plaintiff's and Class members' PII.

82. Defendants' violation of Section 5 of the FTCA constitutes negligence per se.

83. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII by failing to or failing to ensure the third parties they contract with and share PII with, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII to unauthorized individuals.

84. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII would not have been compromised.

85. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; (vii) loss of value of the PII that was compromised in the Data Breach; and (viii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT
Against Pathward Only

86. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

87. Plaintiff brings this claim only against Pathward.

88. In connection with the dealings Plaintiff and Class members had with Defendants, Plaintiff and Class members entered into implied contracts with Pathward.

89. Pursuant to these implied contracts, Plaintiff and Class members provided Pathward with their PII, directly or indirectly, for Pathward to provide services. In exchange, Pathward agreed to, among other things, and Plaintiff and Class members understood that Pathward would: (1) provide services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII; and (3) protect Plaintiff's and Class members' PII in compliance with federal and state laws and regulations and industry standards.

90. The protection of PII was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Pathward, on the other hand. Indeed, Pathward was clear in its representations regarding privacy, and on the basis of those representations Plaintiff and Class members understood that Pathward supposedly respects and is committed to protecting customer privacy.

91. Had Plaintiff and Class members known that Pathward would not adequately protect its customers' and former customers' PII, they would not have provided Pathward with their PII.

92. Plaintiff and Class members performed their obligations under the implied contracts when they provided Pathward with their PII, either directly or indirectly.

93. Pathward breached its obligations under its implied contracts with Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII in a manner that complies with applicable laws, regulations, and industry standards, including by not ensuring that the third parties it contracts with and shares PII with implemented and maintained adequate security protocols and procedures.

94. Pathward's breach of its obligations of the implied contracts with Plaintiff and Class members directly resulted in their PII being affected in the Data Breach and the injuries that Plaintiff and all other Class members have suffered as a result of and in connection thereto.

95. Plaintiff and all other Class members were damaged by Pathward's breach of implied contracts because: (i) they paid—directly or indirectly—for data security protection they did not receive; (ii) they face a substantially increased and imminent risk of identity theft—a risk justifying or necessitating expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII has been breached; (v) they were deprived of the value of their PII, for which there is a well-established national and international market; and (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risk of identity theft they face and will continue to face.

COUNT IV
BREACH OF FIDUCIARY DUTY
Against Pathward Only

96. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

97. Plaintiff brings this claim only against Pathward.

98. Plaintiff and Class members gave Pathward their PII in confidence, believing that Pathward would protect that information. Plaintiff and Class members would not have provided Pathward with this information had they known it would not be adequately protected.

99. Pathward's acceptance and storage of Plaintiff's and Class members' PII created a fiduciary relationship between Pathward and Plaintiff and Class members. In light of this relationship, Pathward must act in good faith primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class members' PII.

100. Due to the nature of the relationship between Pathward and Plaintiff and Class members, Plaintiff and Class members were entirely reliant upon Pathward to ensure that their PII was adequately protected. Plaintiff and Class members had no way of verifying or influencing the nature and extent of Pathward's data security policies and practices or the extent to which it ensured that the third parties it contracts with and shares PII with maintained adequate data security practices and protocols, and Pathward was in an exclusive position to guard against the Data Breach.

101. Pathward has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of their relationship. It breached that duty by, among other things, failing to properly safeguard Plaintiff's and Class members' PII that it collected,

failing to ensure Plaintiff's and Class members' PII was shared with entities with adequate data protection systems and measures in place, and failing to notify Plaintiff and Class members of the Data Breach in a timely manner.

102. As a direct and proximate result of Pathward's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 815 ILCS 505/2, *et seq*. ("ICFA")

103. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

104. Pathward offered and continues to offer banking and other services in the State of Illinois.

105. Plaintiff and Class members purchased and received banking or other services from Pathward for personal, family, or household purposes.

106. Pathward engaged in unlawful and unfair practices in violation of the ICFA by failing to implement and maintain reasonable security measures to protect and secure its

clients' PII in a manner that complied with applicable laws, regulations, and industry standards.

107. Pathward makes explicit statements to its customers that their PII will remain private.

108. Pathward's duties also arise from the Illinois Personal Information Protection Act, 815 ILCS 530/45(a) which requires:

> A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure.

815 ILCS 530/45. Pathward violated this duty by failing to implement reasonably secure data security policies.

109. Pathward further violated the ICFA by failing to notify its current and former patients of the data breach in a timely manner. The Illinois Personal Information Protection Act requires entities that experience a data breach to notify Illinois residents "in the most expedient time possible and without unreasonable delay." 815 ILCS 530/10. Violation of the Illinois Personal Information Protection Act constitutes an unlawful practice under the ICFA. 815 ILCS 530/20.

110. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII. Further, Pathward's failure to adopt reasonable practices in protecting and safeguarding its clients' PII will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk of medical identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for Pathward's practice of collecting and storing PII without appropriate and reasonable safeguards to protect such information.

111. As a result of Pathward's violations of the ICFA, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Pathward's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT

112. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

113. This claim is pleaded in the alternative to the breach of implied contract claim.

114. Plaintiff and Class members conferred a monetary benefit upon Defendants in the form of their valuable PII and through money paid for services, a portion of which Plaintiff and Class members reasonably expected would be used to protect their PII.

115. Defendants accepted or had knowledge of the benefits conferred upon them by Plaintiff and Class members by storing or transferring the PII, or otherwise using it to facilitate their business, and providing services to Plaintiff and Class members.

116. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the loss of value of Plaintiff's and Class members' PII. Plaintiff and Class members also suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures

that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

117. Defendants should not be permitted to retain the money belonging to Plaintiff and Class members because Defendants failed to adequately implement the data privacy and security procedures for themselves that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards. Defendants should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by them as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of the Class, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiff as class representative and undersigned counsel as class counsel;

B. Award Plaintiff and Class members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class members have an effective remedy, including enjoining Defendants from continuing the unlawful practices as set forth above;

D. Award Plaintiff and Class members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiff and Class members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiff and Class members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: October 26, 2023

Respectfully submitted,

/s/ Edward S. Hruska III
Edward S. Hruska III
Bachand & Hruska, P.C.
206 West Missouri Ave.
Pierre, South Dakota 57501
Telephone: 605-224-0461
ehruska@pirlaw.com

Ben Barnow*
Anthony L. Parkhill*
Barnow and Associates, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Telephone: 312-621-2000
Facsimile: 312-641-5504
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff and the Proposed Class

**pro hac vice forthcoming*

JS 44 (Rev. 04/21)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

Jacob Kent

(b) County of Residence of First Listed Plaintiff Rock Island, Illinois
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Edward S. Hruska III; Bachand & Hruska, P.C., 206 West Missouri Ave., Pierre, South Dakota 57501; 605-224-0461

DEFENDANTS

Pathward, N.A., Ipswitch, Inc., and Progress Software Corporation

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☉ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☑ 4
Citizen of Another State	☑ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☉ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☉ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Class action relating to a data breach affecting the customers of Pathward, N.A.

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☉ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
Oct 26, 2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Edward S. Hruska III

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. **Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.